# "MAKING SAFETY HAPPEN" THROUGH PROBABILISTIC RISK ASSESSMENT AT NASA

**Roger L. Boyer[(1)], Teri L. Hamlin[(1)], Warren C. Grant[(1)], Michael A. Stewart[(1)], Robert B. Cross[(1)], James H. Rogers[(2)], Alfred S. Berrios[(3)]**

*[(1)]NASA JSC, 2101 NASA Parkway, Mail Code NC4, Houston, Texas, 77058, USA, Roger.L.Boyer@nasa.gov*
*[(2)]NASA MSFC, Mail Code QD35, Huntsville, Alabama, 35812, USA, James.H.Rogers@nasa.gov*
*[(3)]NASA KSC, Mail Code SA-F, Kennedy Space Center, Florida, 32899, USA, Alfred.S.Berrios@nasa.gov*

## ABSTRACT

NASA is using Probabilistic Risk Assessment (PRA) as one of the tools in its Safety & Mission Assurance (S&MA) tool belt to identify and quantify risks associated with human spaceflight. This paper discusses some of the challenges and benefits associated with developing and using PRA for NASA human space programs. Some programs have entered operation prior to developing a PRA, while some have implemented PRA from the start of the program. It has been observed that the earlier a design change is made in the concept or design phase, the less impact it has on cost and schedule. Not finding risks until the operation phase yields much costlier design changes and major delays, which can result in discussions of just accepting the risk. Risk contributors identified by PRA are not just associated with hardware failures. They include but are not limited to crew fatality due to medical causes, the environment the vehicle and crew are exposed to, the software being used, and the reliability of the crew performing required actions. Some programs have entered operation prior to developing a PRA, and while PRA can still provide a benefit for operations and future design trades, the benefit of implementing PRA from the start of the program provides the added benefit of informing design and reducing risk early in program development.

Currently, NASA's International Space Station (ISS) program is in its 20th year of on-orbit operations around the Earth and has several new programs in the design phase preparing to enter the operation phase all of which have active (or living) PRAs. These programs incorporate PRA as part of their Risk-Informed, Decision-Making (RIDM) process. For new NASA human spaceflight programs discussion begins with mission concept, establishing requirements, forming the PRA team, and continues through the design cycles into the operational phase. Several examples of PRA related applications and observed lessons are included.

## 1. BACKGROUND

The fundamentals of PRA had their start in the early 1960's as a way to evaluate the safety of designing and operating Intercontinental Ballistic Missiles (ICBM's) via fault trees. The approach showed value in identifying and analyzing risks in other industries.

In the early 1960's, NASA used reliability analysis to assess the likelihood of making it to the moon and back safely as President Kennedy stated. However, the results of the assessment revealed a higher risk than NASA believed and abandoned the analysis effort. The program resulted in only one of the lunar excursions failing to meet its mission objectives while returning the crew home safely.

A decade later, the US Nuclear Regulatory Commission (NRC) picked up PRA for the 1975 Reactor Safety Study (RSS).[1] Previously, the Atomic Energy Commission and Nuclear Regulatory Commission (NRC) used Design Basis Accidents (DBAs) to evaluate reactor and plant designs. DBAs are worst case, multiple failure, events. After the study was complete, it was book shelfed. Following the Three Mile Island (TMI) accident in 1979, someone recalled that the RSS revealed a similar scenario. A review of the RSS findings confirmed the scenario and the NRC concluded that PRA had a use in identifying and analyzing potential scenarios at nuclear power plants. Additional studies of other plants were performed, research on methodology improvement resulted in an approach with much more capability. The TMI accident showed that the more likely scenarios had as much or more risk than the worst case scenarios. PRA introduced a best-estimate risk approach to evaluate plant designs and operations instead of DBAs, which assumed worst case scenarios. By 1990, the NRC required every US nuclear power plant (more than 100) to perform an Individual Plant Examination (IPE), which was accomplished using PRA. Some plants attempted to satisfy the IPE using other methods but failed and eventually used PRA to meet the requirement. PRA is used in the nuclear industry to evaluate and improve designs of both already built and

those being built or planned. PRA was shown to be useful in the design process and during operation. Operating procedures and operator training were both improved.

Following the *Challenger* accident in 1986, the Rogers Commission recommended that NASA use PRA to evaluate the Shuttle design and operation.[2] NASA started by applying PRA to evaluate nuclear payload launches for ascent only. Later, a 1995 PRA was performed for ascent and descent operations with minimal in-space application. By 2001, the Shuttle Program sanctioned a full scope PRA that was interrupted by the *Columbia* accident. An independent peer review (IPR) sponsored by NASA's Office of Safety & Mission Assurance (OSMA) was performed in 2003. Recommendations were made and accepted. The Shuttle PRA evolved as post-*Columbia* accident improvements were being added, such as in-space heat shield inspections and repair capabilities.

After the Shuttle program concluded in 2011, the Shuttle PRA was used to evaluate the effectiveness of design changes or upgrades over the life of the program since 1981. The Shuttle PRA showed the estimated risk of flying the Shuttle at the end of program was approximately 1 in 90. Removing each upgrade one mission at a time showed that the risk of flying STS-1 in 1981 was about 1 in 10.[3] In other words, the initial flight risk of the Shuttle was about an order of magnitude greater than it was at the end of the program. This surprised some, but not all. In the early 1980's, it was believed by management that flying the Shuttle was about 1 in 100,000, whereas engineers believed it to be about 1 in 100. Dr. Richard Feynman (the Nobel laureate asked to be a member of the Roger's Commission for the *Challenger* Accident) also pointed out that the estimates that NASA had developed for main engine failure could not possibly be as reliable as quoted.[4] However, not until the Shuttle PRA was performed did anybody have a basis for more realistic estimates. This effort was also very informative to estimate the risk of future first flights when only the mature or design capable risk estimate is known prior to flight.

In February 2008, the Aerospace Safety Advisory Panel (ASAP) pointed out the need to establish risk targets and minimal levels of safety to encourage free discussion among various design participants at both the program level and the safety requirement level. In July 2010, the ASAP was briefed on the three levels of acceptable mission risk. The first level, the Agency Threshold, sets the agency's quantifiable risk tolerance for the program or mission that is required to be reported to the Administrator. The second level, the Program design and mission requirement, sets the "design to" level which allows for margin to the threshold to cover unknowns and uncertainty early in design. The third level, the Agency Long Term Goal, sets the expectation of continuous improvement. In March 2011, OSMA recommended the first Agency Risk Tolerance Thresholds and Goals for an ISS Mission.[5]

## 2. PRA OVERVIEW

PRA is a comprehensive, structured, and disciplined approach to identifying and analyzing risk in engineered systems and/or processes.[6] It attempts to quantify rare event probabilities of failures. It attempts to take into account all possible events or influences that could reasonably affect the system or process being studied. It is inherently and philosophically a Bayesian methodology. In general, PRA is a process that seeks answers to three basic questions:

- What kinds of events or scenarios can occur (i.e., what can go wrong)?
- What are the likelihoods and associated uncertainties of the events or scenarios?
- What consequences could result from these events or scenarios (e.g., Loss of Crew, Loss of Mission, Loss of Hydrocarbon Containment during deep sea oil drilling, Nuclear Reactor Core Damage Frequency)?

Figure 1 shows an overview of the PRA process.

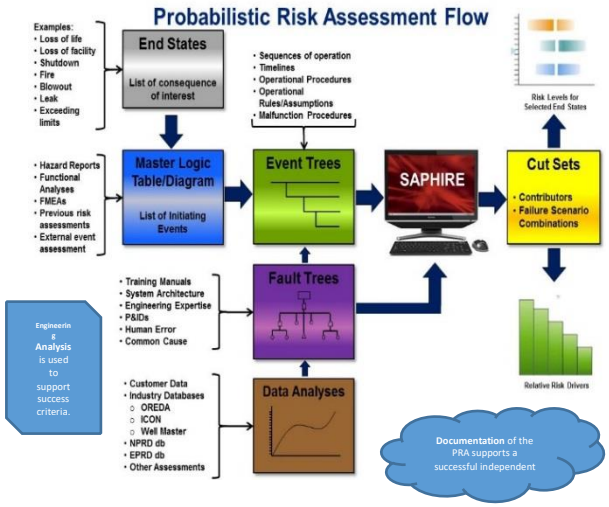


*Figure 1. Probabilistic Risk Assessment Overview*

NASA's OSMA established a procedures guide for the agency.[7] However, it leaves off at a higher level than is needed by each program to implement within the program. Therefore, a more program specific PRA methodology document is established to provide clearer guidance to each program's PRA analysts.

## 3. SPACE SHUTTLE

The Space Shuttle program flew from April 1981 to July 2011. The Space Shuttle was comprised of five elements; Orbiter, Space Shuttle Main Engines (SSMEs), Solid Rocket Boosters (SRBs), Reusable Solid Rocket Motors (RSRMs) and the External Tank (ET). During its 30 year lifetime, the Space Shuttle flew 135 missions to Low Earth Orbit (LEO). Two of those missions resulted in catastrophic events (i.e. *Challenger* and *Columbia* accidents).

Following the *Challenger* accident in 1986, work began on proof of concepts for PRA modeling of selected Shuttle systems followed by "ascent only" assessments in support of nuclear payload missions. In 2001, the Shuttle Program Manager sanctioned a full scope Shuttle PRA (SPRA). Each of the five Shuttle elements was responsible for generating a PRA model of its element, which was to be integrated into the SPRA. By 2003, the baseline was completed and an independent peer review was performed. As increasing fidelity and expansion of the modeling scope occurred over the following years, the SPRA risk varied. The SPRA yielded a mission assessment from T-5 minutes (Orbiter auxiliary power units start) to wheel stop. This evolution is shown in Figure 2. The final mean estimated risk of the Shuttle was 1 in 90 with a 5$^{th}$ percentile of 1 in 127 and a 95$^{th}$ percentile of 1 in 63. The error factor (i.e. Measure of uncertainty) was estimated at 1.4 considering the improvements that had been made, these results were consistent with an empirical calculation of 2 failures in 135 missions which gives a 1 in 68 probability of LOCV.

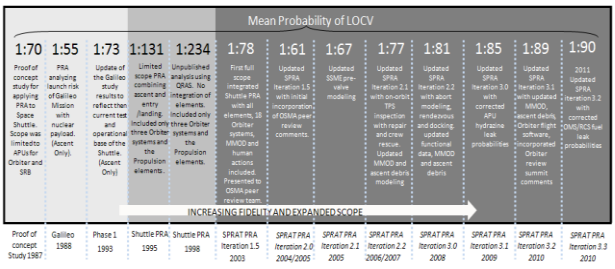


*Figure 2. Shuttle Probabilistic Risk Assessment Development*

Early in the program, two qualitative risk assessments were made. These were not PRAs. The Wiggins Analysis [8] in 1982 put the overall risk of losing a Shuttle between 1 in 500 and 1 in 5000, which was mainly based on engineering judgment. The Weatherwax Analysis [9] in 1983 put the overall risk of losing a Shuttle at 1 in 35. It was a review of the Wiggins analysis with a more data-based approach. The Weatherwax report mentioned Nuclear PRAs and inclusion of other risks such as Common Cause Failures (CCFs) and crew error, which are included in PRAs.

The Space Shuttle program actively used PRA the last half of the program, not as something to meet a requirement but as an indicator of what risks it was facing. Unfortunately, the PRA results were coming out at about the time of the *Columbia* accident in 2003. Following the *Columbia* accident, the Shuttle PRA was completed and used by program management to address the top risk drivers. For example, the Shuttle program manager would start at the top risk driver and work his way down to #10 asking what is being done and what can be done for each risk driver. The Top 8 represented ~80% of the estimated risk in 2003 and by the end of the program in 2011 the Top 10 represented about 70%. There were 97 Shuttle PRA (SPRA) applications and special assessments that were performed by the Shuttle PRA Team (SPRAT) between return to flight from *Columbia* and end of the Shuttle program. Examples of applications and special assessments that utilize the Shuttle PRA include: Hubble Space Telescope Service Mission 4, potential crew rescue of the last mission (STS-135), dual docked operations, emergency de-orbit, and entry overflight risk. Special assessments include: flow control valve, engine cutoff sensor failures, power bus isolation supply, and oscillations of the Orbiter docking system.

To maintain the SPRA as current, it was updated about every year and referred to as Iterations. There were seven Iterations after the baseline in 2003. Each Iteration included an increase in scope and updated data.

Another finding from the Shuttle program PRA was the difference between when the risk was initiated to when it was realized. For example, the thermal protection system (TPS) of the wing leading edge on the Orbiter could be damaged during ascent, but loss of crew would not be realized until re-entry as was the case for the *Columbia* accident. This meant that on-orbit inspection could identify a damaged TPS and allow time to make some repairs. It was not a guarantee as some damages could not be repaired and some could not be detected. This is

important to consider for future spacecraft returning to Earth.

The Shuttle is a very reliable vehicle in comparison with other launch systems. Much of the risk posed by Shuttle operations is related to fundamental aspects of the spacecraft design and the environments in which it operates. It was unreasonable to assume that significant design improvements could be implemented to address these risks in the operations phase of the program versus earlier in the design / development phase. Risk assessments, like the SPRA, could help identify and analyze these contributors early in the design process to determine whether a design change is warranted.

The SPRA provides a cornerstone for future human space programs to benefit from by knowing what can and has been done previously to identify and analyze risk contributors in the continuous risk management process. SSP management viewed the SPRA results as one of many inputs in their risk-informed decision making process.

## 4. INTERNATIONAL SPACE STATION (ISS)

The ISS is a joint program between five participating space agencies: the US National Aeronautical and Space Agency (NASA), Russia's Roscosmos, Japan's JAXA, the European Space Agency (ESA), and the Canadian Space Agency (CSA). The ISS is a space station, or habitable artificial satellite, in low Earth orbit about 250 miles up. The first element of the ISS went up in 1998, with the first long-term residents arriving in November 2000. It has been inhabited continuously for 20 years and expected to operate until 2030. The last pressurized module was added in 2011. It is approximately 250 feet long and 360 feet wide with a habitable volume of approximately 33,000 cubic feet and circling the Earth every 92 minutes at 17,100 mph. It can be seen with the naked eye from Earth. Approximately 240 people from 18 countries have visited it to date and over 2200 experiments have been performed.

Its PRA effort started in 1999. An independent peer review team reviewed the ISS PRA in 2002 and again in 2010 after the PRA was restarted to correct initial issues. Findings were made and incorporated. The scope of the ISS PRA was the complete state of the vehicle and not its construction. It included hardware, medical, and Micrometeoroid and Orbital Debris (MMOD) risks. A fire study was performed in 2011. That established a new methodology to more accurately assess the fire risk to the ISS from all known sources of ignition. Though ultimately the quantified risk value was low, the consequences of fire are extremely high. The PRA analysis enabled the program to identify categories of risk and mitigate potential sources based upon their risk contribution.

The ISS does not have an overall LOC requirement, but does assess the probability of LOC and evacuation as well as several loss of station end states. The PRA is used, similar to SSP, to identify, assess, and mitigate risk. Examples include MMOD studies to mitigate exposure to key components and systems, evaluation of critical failures such as the ammonia heat exchanger that failed and was replaced on orbit, and space vehicle risk as an emergency return option for crew members.

## 5. CROSS PROGRAM

NASA's Cross Program or Exploration Systems Development (ESD) program is currently the integration of three individual NASA programs: Orion, Space Launch Systems (SLS), and Exploration Ground Systems (EGS). Future mission programs may include Deep Space Gateway, lunar lander, etc. Each program has a role in getting NASA back to the moon. Orion is the spacecraft, similar to Apollo. SLS is the launch vehicle, similar to the Saturn V. EGS provides the ground support systems prior to launch and post-landing. Each program is responsible for performing and developing its PRA. Both Orion and SLS have LOC requirements. EGS does not because it was believed to have insignificant risk as compared to Orion and SLS. However, the Cross Program PRA (XPRA) includes EGS to capture the overall risk associated with each mission. The cross program only has one probability of Loss of Crew (LOC) requirement, the combined ascent risk of 1 in 400. Both Orion and SLS have an ascent LOC requirement and Orion has an Entry, Descent, and Landing (EDL) LOC requirement. The XPRA assesses the risk from crew ingress to "boots on deck". Boots on deck is defined here as when the crew is loaded on a vessel or location with complete medical facility (i.e. Not a life raft or helicopter). This requires assessing ground support systems, external events, and the complete mission. Since 2014, the NASA Administrator has established an agency LOC threshold of 1 in 75 for cis-lunar missions [10], such as what EM-1 and EM-2 are planned to fly. EM refers to Exploration Mission. Note that EM-1 is currently planned to be an un-crewed vehicle flying a mission around the moon, thus LOC does not apply. Another end state or top event is used for EM-1, i.e. probability of Loss of Orion Vehicle (LOOV). EM-2 is currently planned to be the first crewed mission. In addition to agency LOC thresholds and program LOC

requirements, the ESD program has also established Technical Performance Measures (TPMs) which provide a "warning track" approach for each major requirement, as shown in Table 1. Therefore, providing a three tiered approach to these LOC requirements. If the estimated risk of any monitored risk rises above the TPM, then a "trip wire" occurs to inform management that estimated risk is approaching the program requirement. If the estimated risk continues to rise above the Program LOC Requirements, management is again flagged to respond. This time action is required. However, if the estimated risk rises above the Agency LOC Threshold, then the NASA Administrator becomes involved to discuss with the program.

| | **Pre-launch and Ascent** | | **In-Space** | | **EDL and Post Landing** | **Mission** |
|---|---|---|---|---|---|---|
| | SLS | Orion | SLS | Orion | Orion | |
| Agency Threshold | 1 in 300 | | 1 in 150 | | 1 in 300 | 1 in 75 |
| ESD Reqmt | 1 in 550 | 1 in 1400 | N/A | N/A | 1 in 650 | TBD |
| ESD TPM Objective | 1 in 400 TPM 1.a | | N/A | N/A | N/A | 1 in 130 TPM 4.a |

*Table 1. ESD Loss of Crew (LOC) Requirements and Technical Performance Metrics (TPM)*

The SLS Block 1 configuration consists of a core stage, solid rocket boosters, and the upper stage. The core stage includes four RS-25s, liquid Hydrogen (LH2) and liquid Oxygen (LO2) tanks. Two solid rocket boosters with five segments each are used for additional thrust during the first ~120 seconds of ascent. The Block 1 upper stage, which is referred to the Interim Cryogenic Propulsion Stage (ICPS), is a liquid oxygen / liquid hydrogen ($LO_2/LH_2$) based system that performs the Perigee Raise Maneuver (PRM). Orion's service module will perform the Trans-Lunar Injection (TLI) burn for EM-2.

SLS's LOC requirement is 1 in 550 and 1 in 85 for ascent probability of Loss of Mission (LOM). SLS LOM means that SLS cannot achieve the mission objective and Orion is now challenged to escape and safely return via its launch abort system. The SLS is essentially divided into core stage and upper stage. The core stage takes the vehicle from launch pad to ~8.5 minutes into ascent. The upper stage covers the rest of ascent and depending on the mission profile into a LEO or TLI burn.

The SLS PRA is used to verify its LOC requirements as well as for several trade studies to help ensure that it meets its requirements. A couple of examples of these trade studies are MMOD risk reduction, abort triggers, and alternate Main Engine Cutoff (MECO) targets. SLS performed a trade study on MMOD risk reduction trades for both EM-1 and EM-2. PRA was used for trigger selection and evaluation of abort triggers, which included adding a command authority trigger to protect the crew against an all TVC hard over failure. Another crew safety possibility would be the alternate MECO target to allow reaching a safe orbit in the case of an engine shutdown. PRA shows benign liquid engine shutdown to be one of the risk drivers. PRA was a key tool for adding redundancy to the SLS systems.

The Orion Program provides the Orion spacecraft, which consist of a Crew Module (CM), a Service Module (SM), a Spacecraft Adaptor (SA), and a Launch Abort System (LAS). The SM is comprised of two subcomponents: the Crew Module Adapter (CMA) and the European Service Module (ESM). The ESM is provided by the European Space Agency (ESA). Lockheed Martin (LM) provides the other Orion components.

- The Orion CM is a pressurized, crewed element that houses the crew members from lift-off to lunar orbit and brings the crew members safely back to the Earth's surface at the end of a mission. The Orion CM provides all services necessary to support the crew members while onboard for the EM-2 mission.
- The ESM, which is attached to the CM by the CMA, provides services to the CM in the form of propulsion, consumables storage, heat rejection, and power generation. The Orion provides power and data interfaces for unpressurized cargo and secondary payloads within the SM.
- The LAS provides an abort capability to safely transport the CM away from the launch vehicle stack in the event of an emergency on the launch pad or during the first few minutes of ascent. The LAS is jettisoned after the SM fairings have been safely jettisoned.

Orion's LOC requirements are 1 in 1400 for ascent and 1 in 650 for EDL. The Orion PRA was used for several risk trade studies during its development. For example, the PRA was used to evaluate the comparative risk between SM serial and parallel propulsion systems, provide risk rankings for various docking system designs, and to evaluate cross connection capabilities in the fuel supply section of the propulsion system.

The EGS Program provides the systems and capabilities to process, launch and then recovery of the Orion spacecraft and crew after landing. For this analysis, only the systems involved in launch preparation, launch and recovery are analyzed; these include the following.

- At the launch pad, EGS Ground Support Equipment systems risk are quantified during SLS vehicle final cryogenic propellant servicing, through launch countdown, and launch from Launch Complex 39 Pad B at the Kennedy Space Center.
- For recovery, either following a nominal mission or an abort, EGS provides capabilities to locate, rescue, and transport the spacecraft and crew after landing.

EGS has no LOC requirement, however a PRA is performed to understand the program's mission risk related to both pre-launch and post-landing. EGS's LOC risk includes ground operations performed while the crew is on board during pre-launch, abort rescue operations, and nominal post-landing rescue operations. PRA was used to assist in preliminary emergency egress system design and operations, as well as landing and rescue operations for both nominal and off-nominal conditions. Off-nominal refers to ascent and in-space aborts. In other words, will the crew be landing in the Atlantic, Indian, or Pacific Ocean?

## 6. COMMERCIAL CREW

The Commercial Crew Program (CCP) began in 2010 with the intent to develop commercial partnerships to transport astronauts to the ISS. There are currently two partners (Boeing and SpaceX) developing spacecraft with initial crewed test flights to be launched in 2019. SpaceX launched an un-crewed mission to ISS in March 2019. Each spacecraft will eventually dock to ISS and remain there for around six months and return the crew safely to Earth.

Each partner is responsible for developing a PRA to capture LOC and LOM end states. LOC includes faults initiated by the Crew Transportation System (CTS) from the beginning of crew ingress, prior to launch, through crew egress during rescue. The CTS is the collection of all space-based and ground-based systems (encompassing hardware and software) used to conduct space missions or support activity in space, including, but not limited to, the integrated space vehicle, space-based communication and navigation systems, launch systems, and mission/launch control. LOM includes faults initiated by the CTS which lead to an ascent abort or termination of the mission earlier than the pre-launch planned end of mission timeframe, stranding the crew on ISS requiring a rescue vehicle, inability to dock with the ISS and LOC.

CCP utilizes the PRA for verification of LOC and LOM requirements. CCP LOC and LOM requirements were established based upon Constellation LOC and LOM requirements at the end of the program. Constellation LOC requirements were derived based upon a combination of engineering judgement, Shuttle PRA, and initial estimates of Orion risks. There were two separate LOC requirements set: an overall LOC requirement of 1 in 270 and an Ascent plus Entry LOC requirement of 1 in 500. The Constellation LOM requirement was based upon Soyuz LOM estimates and the ISS Program's desire to be as good as Soyuz. In addition, separate agency thresholds of 1 in 150 for overall mission risk and 1 in 300 for Ascent plus Entry risk was established in 2011 for an ISS mission and applied to both NASA programs conducting such missions and commercial crew transportation.[5] Each partner produced a list of their top risk drivers and compared their overall risk estimate to the program requirement.

## 7. GATEWAY

Gateway is a planned lunar orbital space habitat. Its purpose is to provide a staging platform for lunar operations and for future deep space missions, such as to Mars. As of April 2019, Gateway is made up eight of elements and modules: the Power and Propulsion Element (PPE), the European System Providing Refueling Infrastructure and Telecommunications (ESPRIT)/US Utilization Module, an International Habitat (International Partner Habitation (I-HAB) Module), a domestic habitat (US-HAB Module), an Airlock, Logistics Modules, and a Robotic Arm as shown on Figure 3.

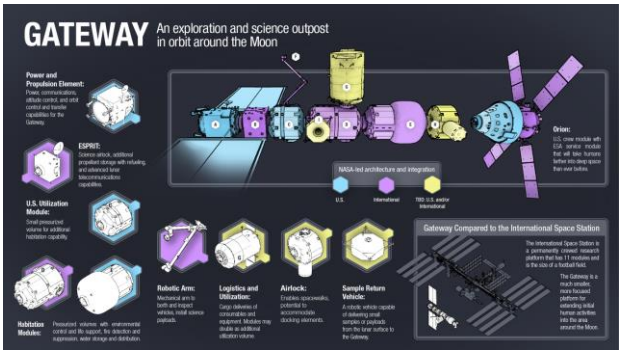


*Figure 3. Current Gateway Architecture*

The Gateway PRA is being developed by NASA at the Gateway Program level so that a consistent PRA methodology will be utilized across modules and elements. The PRA will evaluate both LOC and LOM. LOC includes Gateway initiated faults from crew entering the Gateway approach ellipsoid to crew departure from Gateway ellipsoid. The approach ellipsoid is a designate area around Gateway centered on the Gateway center of mass. Initiated by Gateway includes external events which result in Gateway failure (e.g. MMOD, radiation, etc.) and includes human error associated with operating Gateway but excludes events initiated by Orion which are captured in Orion LOC and LOM estimates (e.g. docking event initiated by Orion). Crew medical risk is planned to be covered at the mission level including both Orion and Gateway. The Gateway Preliminary PRA was created to help establish LOC and LOM requirements, as was done for the Cross Program, and to help with early design trades. The Gateway Preliminary PRA utilizes ISS PRA, Orion PRA and satellite reliability analysis as surrogates for the Gateway systems. It is not a detailed model of Gateway as there are no specific designs to evaluate. As the design matures, a more detailed PRA will evolve to eventually be used to verify LOC and LOM requirements at the program level.

The Gateway program is taking a new approach to LOC and LOM requirements by not allocating LOC and LOM requirements to elements/modules. Instead Gateway is allocating hardware reliability requirements which are consistent with Gateway LOC and LOM requirements. The Gateway elements are required to provide PRA support information necessary to perform the PRA which includes the reliability data as well as supporting the Gateway PRA working group. This approach was proposed based upon a lesson learned from CCP. Since the Program is responsible for meeting the LOC requirement, there is a risk that the elements/modules could meet the hardware reliability requirements but the Program is not meeting LOC or LOM requirements. This risk is believed to be low because of the way the requirements were derived and was accepted by the Program. Although LOC and LOM requirements were proposed for Gateway as part of the Gateway Formulation Sync Review (FSR), they are currently "To Be Resolved" (TBR) pending resolution of the Agency LOC threshold and confirmation of achievability of the Element hardware reliability requirements.

In addition to helping set the LOC, LOM and hardware reliability requirements, the preliminary PRA has been used to perform early design trades. An example of this is the evaluation of Thermal Control System (TCS) architecture options including single and dual loop configurations with both fluid and heat exchanger cross-strapping capability. Another example included evaluating the impact of providing a self-rescue capability for Gateway Extravehicular Activities (EVAs).

Due to the planned operational approach with Gateway, only periodically crewed but mainly un-crewed, evaluating maintenance and repair may be a challenge. Capability to perform robotic maintenance and repair is being explored. When integrating Gateway risks into the Cross-Program PRA, the PRA model needs to capture the potential degraded state of Gateway at launch of Orion. This is a new challenge since all other NASA PRAs have assumed that the vehicle is fully operational at beginning of a mission. This capability could help identify if additional Launch Commit Criteria (LCC) are needed to address Gateway failures.

## 8. FUTURE HUMAN SPACE PROGRAMS

Work is already beginning on the human and robotic lunar landers. PRA is planned for the human lander, not sure what will be done for the robotic lander. Eventually, a lunar base may occur in order to provide a more substantial presence on the moon in preparation for missions to Mars. Work is getting exciting, as well as challenging.

It is proposed that NASA continue to use PRA to help identify, quantify, and mitigate risks for future space missions during the concept, design, and operational phases. PRA provides a systematic approach to looking at what can go wrong (how things fail) and the corresponding likelihood of these failure scenarios. Human space exploration faces an enormous number of scenarios that could result in catastrophe. PRA is one of the tools that NASA uses to help improve the likelihood of mission success by identifying and ranking the risks for management to make risk-informed decisions.

Each human space program after the Space Shuttle Program has yielded leadership with differing views of PRA and its use. The process is valid, if performed consistently. Consistency varies by how programs are established and the PRA team gets divided and biased to produce a PRA. Forward plans should produce PRAs at higher levels to allow consistency as well as promote reliability analysis at the lower/project/element levels. PRA is not the answer to all questions, but it is a valuable tool for design and operations.

Several lessons have been derived from human space program PRA development and applications to date. I can't say they were all learned, since each of the follow-on programs didn't use some of them until now with Gateway.

- **Establish project management and funding through the same path.** If you don't, your team will have different bosses thus you will not have a team!

- **Establish a single overall PRA technical authority.** Don't call desired methods as guidelines, if you want the team to follow them. Admiral Hyman Rickover (US Navy) often stated that "Responsibility is a unique concept... You may share it with others, but your portion is not diminished. You may delegate it, but it is still with you... If responsibility is rightfully yours, no evasion, or ignorance or passing the blame can shift the burden to someone else. Unless you can point your finger at the man who is responsible when something goes wrong, then you have never had anyone really responsible." [11]

- **Begin with the end in mind, which sounds simple but is difficult to implement.** Get the Hazard analysis, Failure Modes and Effects Analysis (FMEA), and PRA teams working together versus answering the same questions with different approaches in separate silos or divisions. Mission phase definition is very important as the number of potential phases increases the complexity of the model orders of magnitude. For example, abort modeling from ascent to on-orbit initiated. A functional hazard analysis appears to be a good way to coordinate between hazard and PRA teams, but NASA still needs to demonstrate that from beginning to end.

- **Document, document, document (capture the basis of the PRA) provide traceability (the rabbit trail) of assumptions to results, if you wait to document after presenting the results you will be embarrassed as a minimum.** Have you ever wondered what you did yesterday, last week, last year? That's the first reason why we document! Second, you always find mistakes and/or holes/gaps when documenting your work because you're thinking it through clearer and more focused. The sooner you do this, the quicker you arrive at a reasonable and defendable assessment. Point to the engineering or design analysis that supports your assumptions. If they don't exist, then have the domain expert that told you to make that assumption to state and defend the case instead of the analyst. This keeps the right people involved. Finally, some PRA teams farm out work to third parties. If the third party doesn't document what they did and why, then the primary team will most likely not understand its basis and lead to poor decisions.

- **Get buy in from domain experts early (i.e. before going to present to management).** Start with a good analysis team made up of domain experts (e.g. subsystem engineers, operators / crew, life scientists, external event experts, fire / explosion experts, etc.) and experienced analysts (system modelers, data analysts, integration modelers, human / software analysts, etc.) as needed. This produces the failure logic and data inputs. Go over the failure logic, data, and results with the original team, then share with an independent set of domain experts to ensure that it is defendable as a best-estimate (not conservative or optimistic). Now when you arrive in front of management, the team presents and defends the assessment as one instead of the PRA analyst alone.

- **Start the independent peer review process up front by reviewing the plan with them, then coming back later to ensure that the plan was followed correctly. (Plan your work, work your plan).** The peer review should cover both the scope/content of the PRA (the domain being modeled) as well as the PRA methodology to be used. Make sure you are ready for the peer review.

- **Configuration control should be initiated when the PRA is initiated.** PRA's are designed and developed via an iterative process as knowledge and data is gained, thus there will be several versions along the way. Keep track of what goes into each version (input) and the corresponding output (results). As designs and information changes, so does the PRA. This is why you hear "Living PRA".

- **PRA is a specialized field and that for those not familiar with performing PRA, it takes years to develop the expertise needed.** Significant time can be wasted during the critical time between the Preliminary Design Review and Critical Design Review where PRA could be utilized to inform design decisions. It is important to have an experienced team from the beginning performing the PRA.

We are still learning and trying to improve. Our challenge is communication between analysts, engineering, operations, and management. Analysts need to talk and

be consistent across systems, elements, and programs. This becomes hampered when multiple organizations and companies are involved and on different sides of the requirements fence. Engineering, operations (ground and flight), and health/medical are the domain experts that work with the analysts to comprise the "Analysis Team". Together, these team members access the vehicle/mission/crew to perform the mission PRA. As a result, the Team goes to management to share what has been learned and answer management's questions as to what can be done to reduce risk.

Human space travel and exploration is a risky business. The probability of losing the crew associated with launching from and returning to Earth with current technology is on the order of 1 in 100 to 1 in 200 with minimal in-space activity. As mission duration, number of dockings and landings (mission complexity), number of EVAs and the number of crew increases, the risk increases. Estimates can and are being made to help guide mission architecture and vehicle design. The question is how much risk is too much or acceptable. It depends on the mission objectives, e.g. flying to low Earth orbit, landing on the moon, or landing on Mars. As we go beyond LEO, ascent and descent from Earth becomes a lower risk contributor to overall mission risk. NASA uses a risk-informed decision-making process. Knowing what is acceptable risk, establishes requirements. Using PRA to estimate the expected risk to establish those requirements helps ensure that they are reasonable and achievable. Space mission risk is more than hardware related. It includes the environment (e.g. MMOD, radiation), the crew (e.g. human reliability, health), and software reliability as automation increases. Underappreciated risks can be best addressed by qualified and unbiased PRA teams. The challenge will always be identifying and addressing unknown-unknown risks before they are realized. Risk analysts, mission planners, and system/vehicle designers must be vigilante and well informed to take us "safely" to the next level of human space missions. Risk averse and risk taking are consistently being addressed as we pick up where we left off 50 years ago and return to working on the moon and beyond.

## 9. REFERENCES


1. Reactor Safety Study – An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants. WASH-1400. NUREG-75/014. U.S. Nuclear Regulatory Commission. October 1975.
2. Report to the President by the Presidential Commission on the Space Shuttle *Challenger* Accident (June 6, 1986). Letter to the President of the United States from Chairman of the Commission William P. Rogers.
3. Hamlin, T., J. Kahn, and Y. Lo (2013). Shuttle Risk Progression by Flight, NASA SSMA-11-001, Rev.1.
4. Feynman, Richard Phillips (2001). What Do You Care What Other People Think? Part 2: Mr. Feynman Goes To Washington: Investigating the Space Shuttle *Challenger* Disaster. W.W. Norton & Company, Inc. 500 Fifth Avenue, New York, N.Y. 10110.
5. Bolden, C.F. (May 17, 2011). Decision Memorandum for the Administrator, Agency's Safety Goals and Thresholds for Crew Transportation Missions to the International Space Station (ISS).
6. https://en.wikipedia.org/wiki/Probabilistic_risk_assessment
7. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners. NASA/SP-2011-3421. Second Edition. December 2011.
8. Wiggins, J.H., (1981). Space Shuttle Range Safety Analysis, Technical Report 81-1329 prepared for NASA Kennedy Space Center.
9. Weatherwax, R.K. and Colglazier, E. W. (1983) Review of Shuttle/Centaur Failure Probability Estimates for Space Nuclear Mission Applications, Sierra Energy and Risk Assessment.
10. Bolden, C.F. (May 27, 2014). Decision Memorandum for the Administrator, Agency's Safety Thresholds for Crew for the Human Cis-Lunar Missions.
11. "The Rickover Effect" by Theodore Rockwell, 1992. https://www.azquotes.com/quote/714514